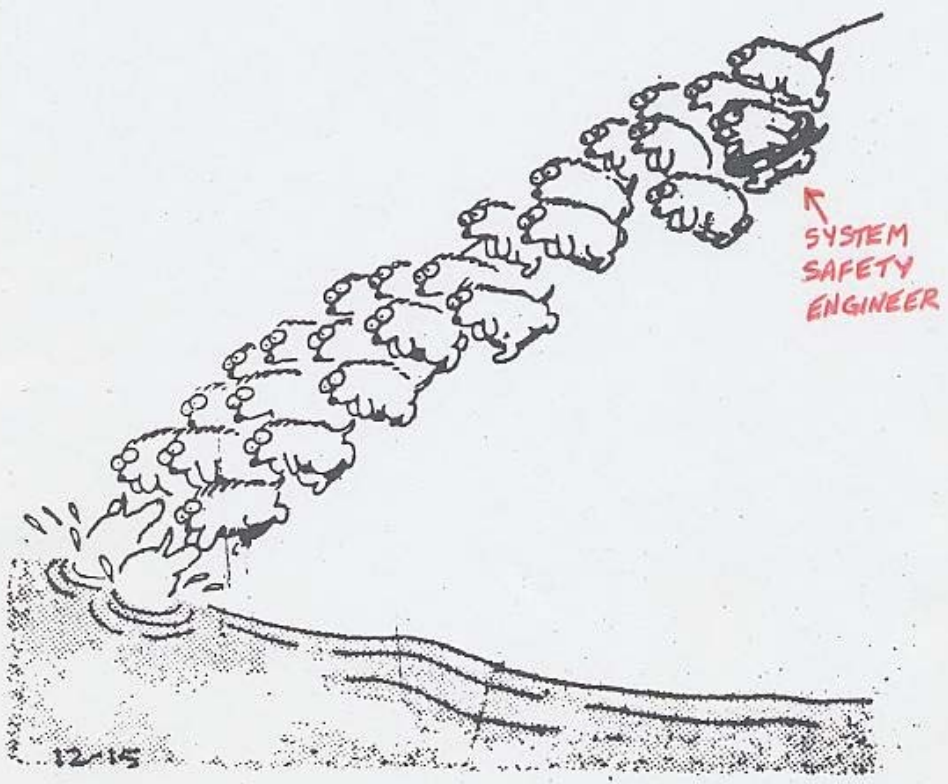
Managing Technical Risk and the Safety Culture on Your Project

Nancy Leveson
Massachusetts Institute of Technology

USRA Center for Program/Project Management Research

The Far Side

By Gary Larson



STAMP: A Formal, Rigorous Approach to Risk Management

- New, more powerful approach to system safety engineering and risk management based on systems theory and control theory rather than reliability (failure) analysis
- Uses formal static and dynamic models
- Provides technical risk analysis and detection of drift toward states of high risk

The Goal

- Risk management tools to
  - Identify organizational risk factors
  - Design and evaluate potential policy and structural improvements
  - Identify leading indicators of increasing or unacceptable risk (“canary in the coal mine”)
  - Provide the information needed for effective and safe decision-making

Chain-of-Events Accident Causality Models

- Explain accidents in terms of multiple events, sequenced as a forward chain over time.
- Events linked together by direct relationships (ignore indirect, non-linear relationships).
- Events almost always involve component failure, human error, or energy-related events.
- Form the basis for most safety-engineering and reliability engineering analysis (FTA, FMEA, PRA) and design.

Limitations of Event-Chain Causality Models

- Social and organizational factors
- System accidents
- Software Error
- Human Error
  - Cannot effectively model human behavior by decomposing it into individual decisions and actions and studying it in isolation from
    - physical and social context
    - value system in which it takes place
    - dynamic work process
- Adaptation
  - Major accidents involve systematic migration of organizational behavior to higher levels of risk.

Migration toward Accidents

- Most major accidents result from drift toward states of high risk
  - Risk increases slowly and nobody notices (“boiled frog phenomenon”)
  - Confidence and complacency increase at same time as risk
  - Challenge in preventing accidents is to establish safeguards to prevent drift and metrics to detect when it is occurring

A Systems Theory Model of Accidents

- Accidents arise from interactions among humans, machines, and the environment.
  - Not simply chains of events or linear causality, but more complex types of causal connections.
- Safety is an emergent property that arises when components of system interact with each other within a larger environment.
  - A set of constraints related to behavior of components in system enforces that property.
  - Accidents when interactions violate those constraints (a lack of appropriate constraints on the interactions).
  - Software as a controller embodies or enforces those constraints.

A Systems Theory Model of Accidents (3)

- Views accidents as a control problem

  e.g., O–ring did not control propellant gas release by sealing gap in field joint

  Software did not adequately control descent speed of Mars Polar Lander.

- Events are the result of the inadequate control

  Result from lack of enforcement of safety constraints

- To understand accidents, need to examine control structure itself to determine why inadequate to maintain safety constraints and why events occurred.

Not a "blame" model – trying to understand "why"

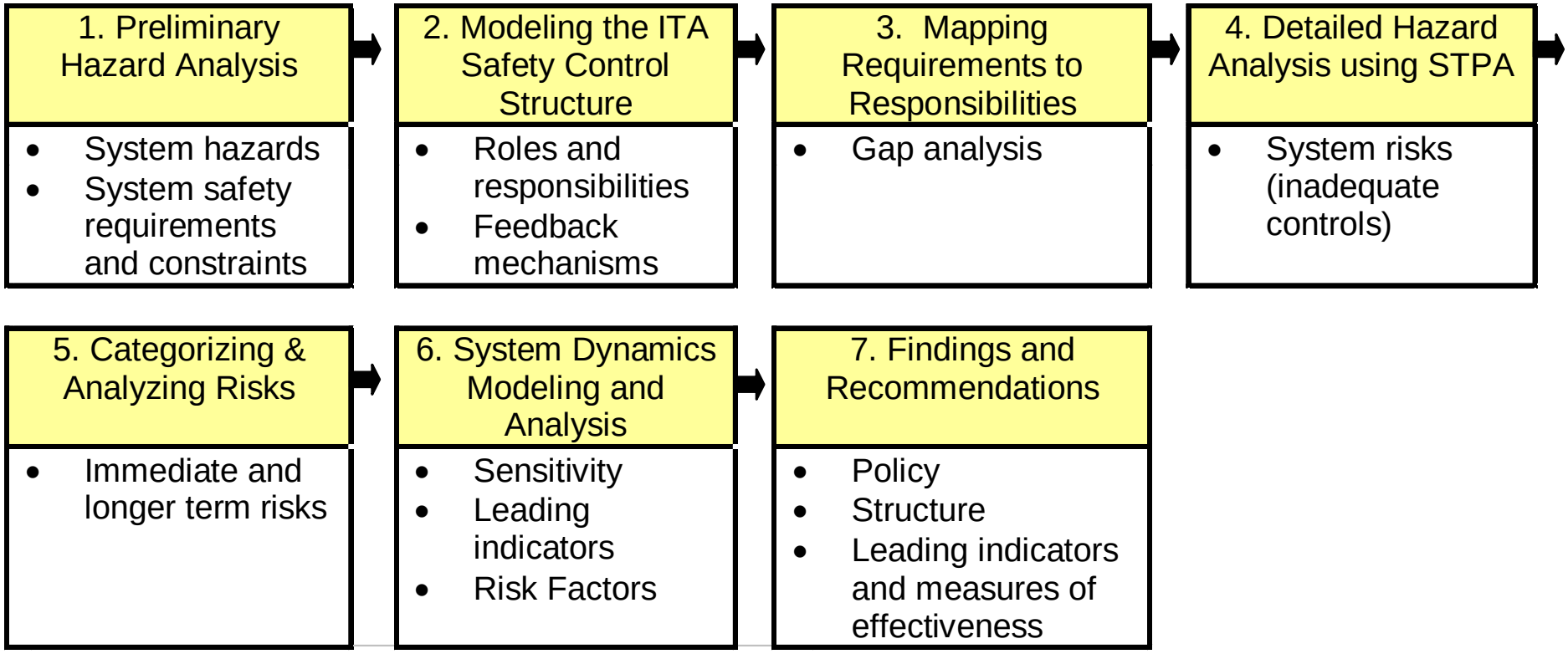
A Systems Theory Model of Accidents

- Systems should not be treated as a static design
  - A socio–technical system is a dynamic process continually adapting to achieve its ends and to react to changes in itself and its environment
  - Preventing accidents requires designing a control structure to enforce constraints on system behavior and adaptation.

STPA: A New Hazard Analysis Technique

- HA technique to support STAMP
- Identify potential control actions that could lead to hazardous system states.
  - A required control action is not provided
  - An incorrect or unsafe control action is provided
  - A potentially correct control action provided too late (at the wrong time)
  - A correct control action is stopped too soon.
- Use control theory concepts to identify risks

The Process


1. Preliminary Hazard Analysis
• System hazards
• System safety requirements and constraints
2. Modeling the ITA Safety Control Structure
• Roles and responsibilities
• Feedback mechanisms
3. Mapping Requirements to Responsibilities
• Gap analysis
4. Detailed Hazard Analysis using STPA
• System risks (inadequate controls)
5. Categorizing & Analyzing Risks
• Immediate and longer term risks
6. System Dynamics Modeling and Analysis
• Sensitivity
• Leading indicators
• Risk Factors
7. Findings and Recommendations
• Policy
• Structure
• Leading indicators and measures of effectiveness

1. Preliminary Hazard Analysis

System Hazard: Poor engineering and management decision-making leading to an accident (loss).

System Safety Requirements and Constraints:

1. Safety considerations must be first and foremost in technical decision-making.
2. Safety-related technical decision-making must be done by eminently qualified experts with broad participation of the full workforce.
3. Safety analyses must be available and used starting in the early acquisition, requirements development, and design processes and continuing through the system lifecycle.
4. The Agency must provide avenues for full expression of technical conscience and a process for full and adequate resolution of technical conflicts as well as conflicts between programmatic and technical concerns.

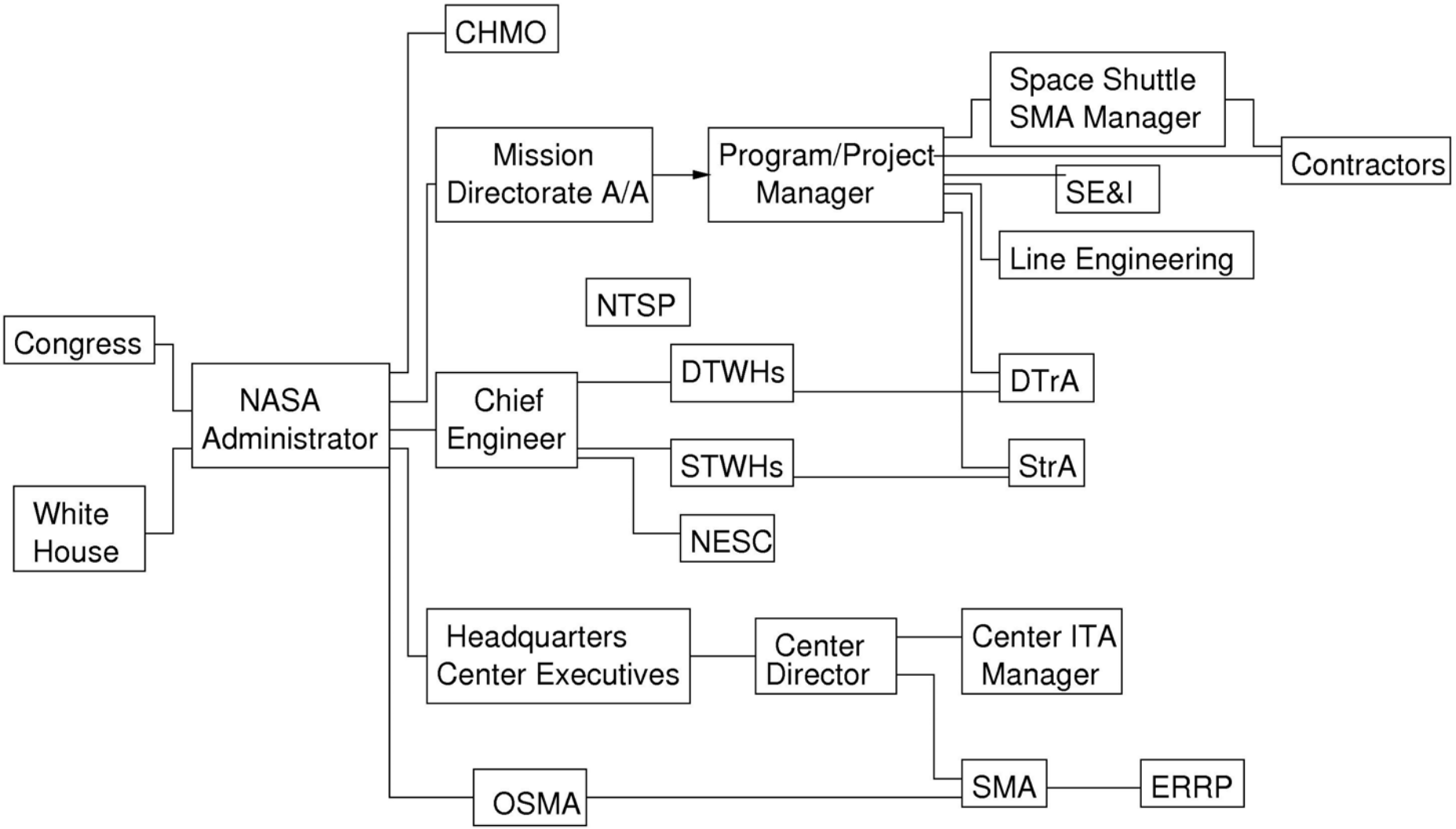
Each of these was refined, e.g.,

1. Safety considerations must be first and foremost in technical decision-making.
   a. State-of-the art safety standards and requirements for NASA missions must be established, implemented, enforced, and maintained that protect the astronauts, the workforce, and the public.
   b. Safety-related technical decision-making must be independent from programmatic considerations, including cost and schedule
   c. Safety-related decision-making must be based on correct, complete, and up-to-date information.
   d. Overall (final) decision-making must include transparent consideration of both safety and programmatic concerns.
   e. The Agency must provide for effective assessment and improvement in safety-related decision-making.

…

To create a set of system safety requirements and constraints sufficient to eliminate or mitigate the hazard

2. Model the ITA Control Structure



For each component specified:

- Inputs, outputs
- Overall role and detailed responsibilities (requirements)
- Potential inadequate control actions
- Feedback requirements

For most added:

- Environmental and behavior-shaping factors (context)
- Mental model requirements
- Controls

Example from System Technical Warrant Holder

1. Establish and maintain technical policy, technical standards, requirements, and processes for a particular system or systems.
   a. STWH shall ensure program identifies and imposes appropriate technical requirements at program/project formulation to ensure safe and reliable operations.
   b. STWH shall ensure inclusion of the consideration of risk, failure, and hazards in technical requirements.
   c. STWH shall approve the set of technical requirements and any changes to them
   d. STWH shall approve verification plans for the system(s)

3. Map System Requirements to Component Responsibilities

- Took each of system safety requirements and traced to component responsibilities (requirements)
- Identified omissions, conflicts, potential issues
- Recommended additions and changes
- Added responsibilities when missing in order for risk analysis to be complete.

4. Hazard Analysis using STPA

General types of risks for ITA:

1. Unsafe decisions are made by or approved by ITA
2. Safe decisions are disallowed (overly conservative decision-making that undermines the goals of NASA and long-term support for ITA)
3. Decision-making takes too long, minimizing impact and also reducing support for ITA
4. Good decisions are made by ITA, but do not have adequate impact on system design, construction, and operation

Applied to each of component responsibilities

Identified basic and coordination risks

Example from Risks List

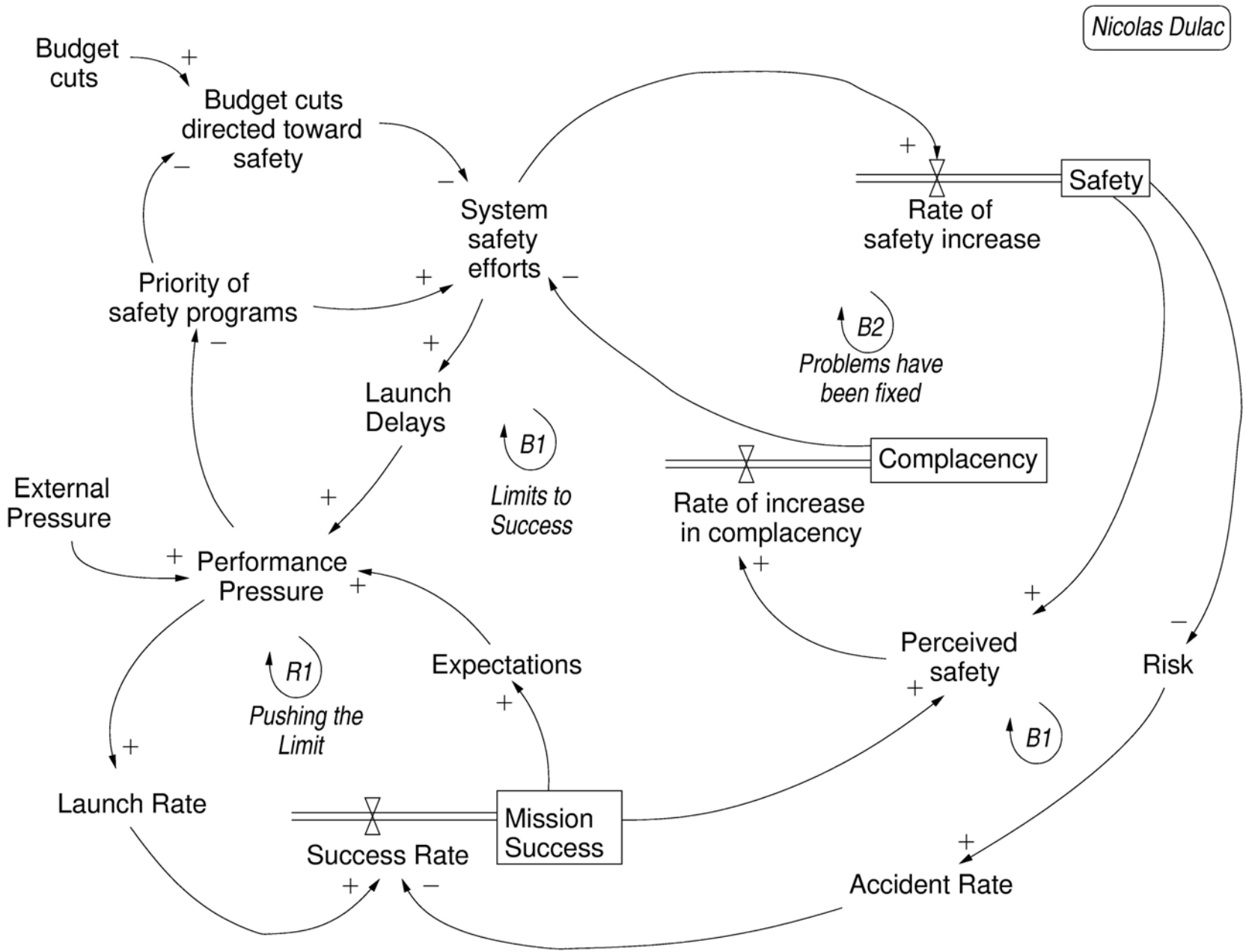
CE Responsibility: Develop, monitor, and maintain technical standards and policy

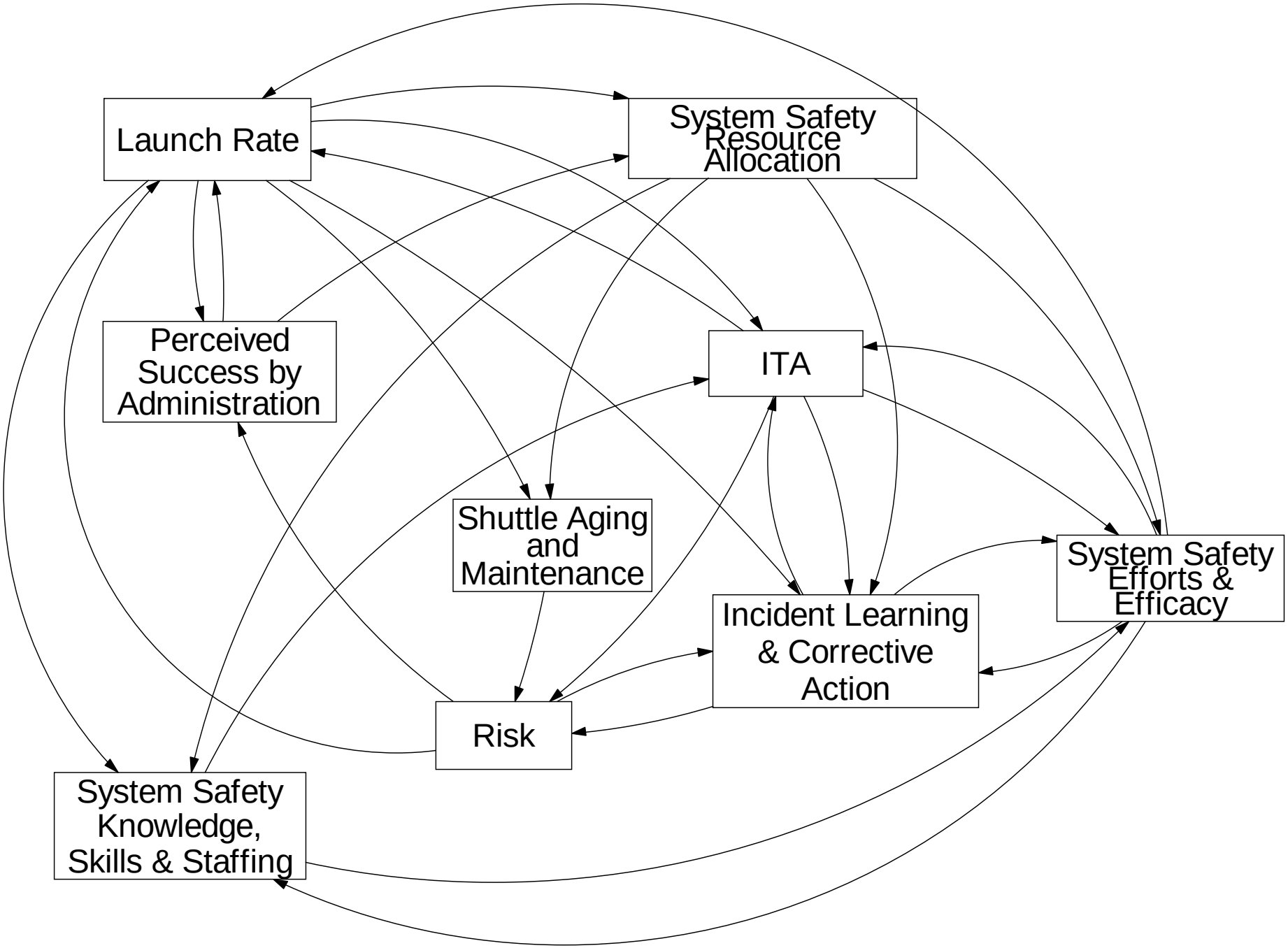
Risks:

1. General technical and safety standards and requirements are not created (IC)
2. Inadequate standards and requirements are created (IC)
3. Standards degrade as changed over time due to external pressures to weaken them. Process for approving changes is flawed (LT).
4. Standards not changed or updated over time as the environment changes (LT).

5. Categorize and Analyze Risks

- Large number resulted so:
  - Categorized risks as
    - Immediate concern
    - Longer-term concern
    - Standard Process
  - Used system dynamics models to identify which risks were most important to assess and measure
    - Provide most important assessment of current level of risk
    - Most likely to detect increasing risk early enough to prevent significant losses (leading indicators)


Nicolas Dulac
Budget cuts
Budget cuts directed toward safety
System safety efforts
Rate of safety increase
Safety
Priority of safety programs
Launch Delays
B2
Problems have been fixed
B1
Limits to Success
Complacency
Rate of increase in complacency
External Pressure
Performance Pressure
Perceived safety
Risk
R1
Pushing the Limit
Expectations
B1
Launch Rate
Mission Success
Success Rate
Accident Rate


Launch Rate
System Safety Resource Allocation
Perceived Success by Administration
ITA
Shuttle Aging and Maintenance
System Safety Efforts & Efficacy
Incident Learning & Corrective Action
Risk
System Safety Knowledge, Skills & Staffing

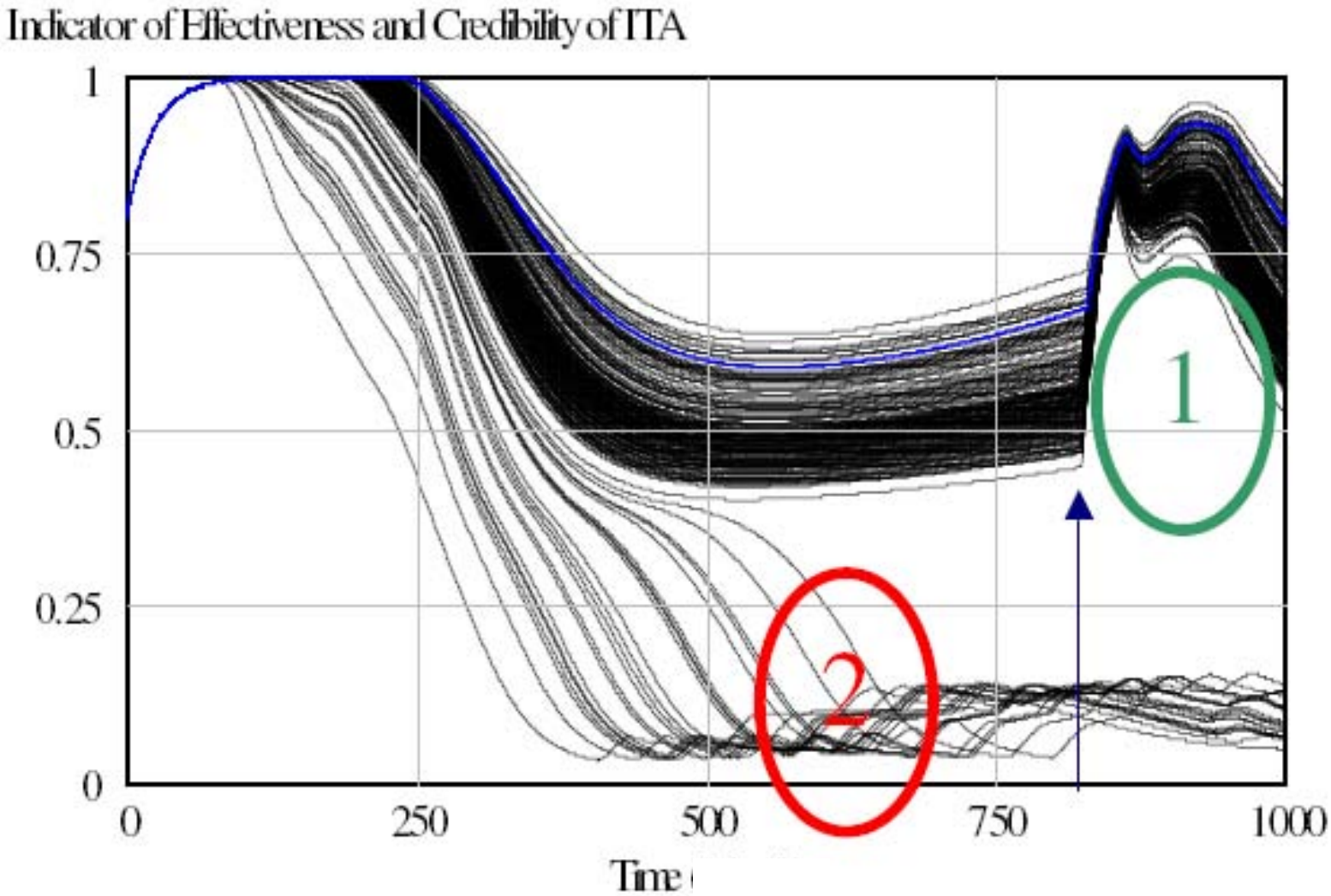
6. System Dynamics Modeling

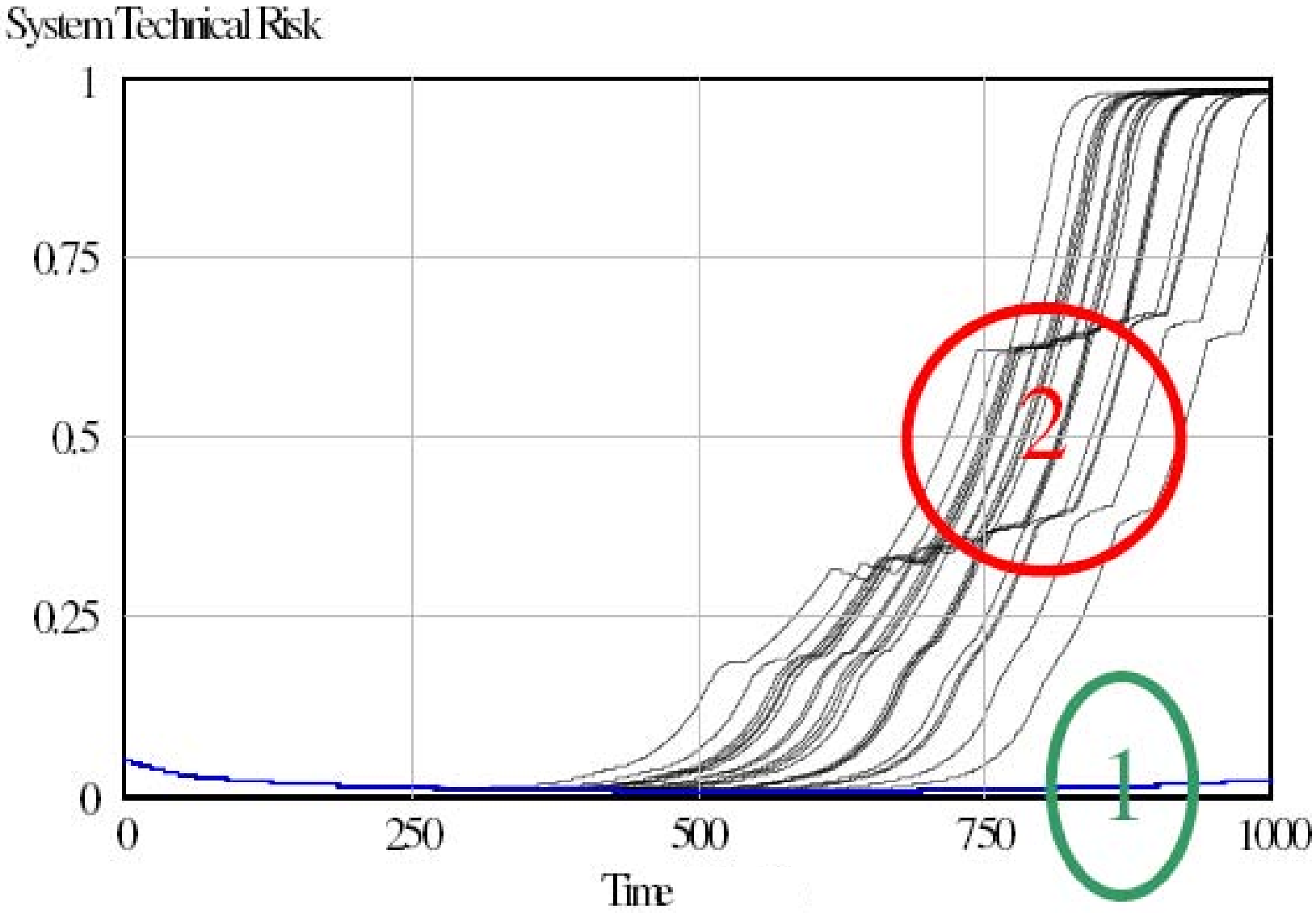
- Modified our NASA manned space program model to include Independent Technical Authority (ITA)
- Independently tested and validated the nine models, then connected them
- Ran analyses:
  - Sensitivity analyses to investigate impact of various parameters on system dynamics and risk
  - System behavior mode investigation
  - Metrics evaluations
  - Additional scenarios and insights

Example Result

- ITA has potential to significantly reduce risk and to sustain an acceptable risk level
- But also found significant risk of unsuccessful implementation of ITA that needs to be monitored
  - 200-run Monte-Carlo sensitivity analysis
  - Random variations of +/- 30% of baseline exogenous parameter values

Sensitivity Analysis Results




System Technical Risk
1
0.75
0.5
0.25
0
0
250
500
750
1000
Time
2
1

Successful Scenarios

- Self-sustaining for short period of time if conditions in place for early acceptance.
- Provides foundation for a solid, sustainable ITA program implementation under right conditions.
- Successful scenarios:
  - After period of high success, effectiveness slowly declines
    - Complacency
    - Safety seen as solved problem
    - Resources allocated to more urgent matters
  - But risk still at acceptable levels and extended period of nearly steady-state equilibrium with risk at low levels

Unsuccessful Implementation Scenarios

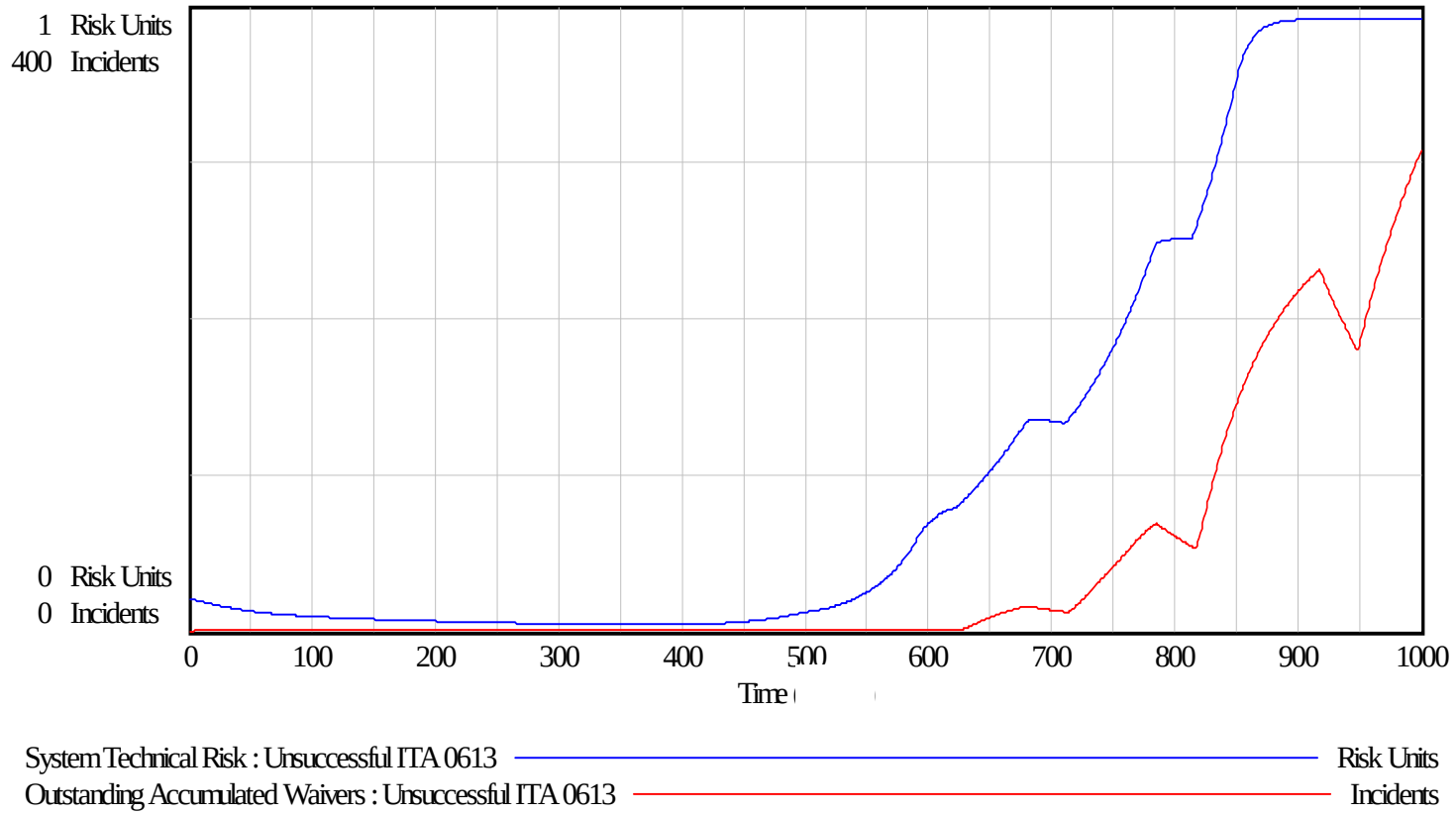
- Effectiveness quickly starts to decline and reaches unacceptable levels
  - Limited ability of ITA to have sustained effect on system
  - Hazardous events start to occur, safety increasingly perceived as urgent problem
  - More resources allocated to safety but TA and TWHs have lost so much credibility they cannot effectively contribute to risk mitigation anymore.
  - Risk increases dramatically
  - ITA and safety staff overwhelmed with safety problems
  - Start to approve an increasing number of waivers so can continue to fly.

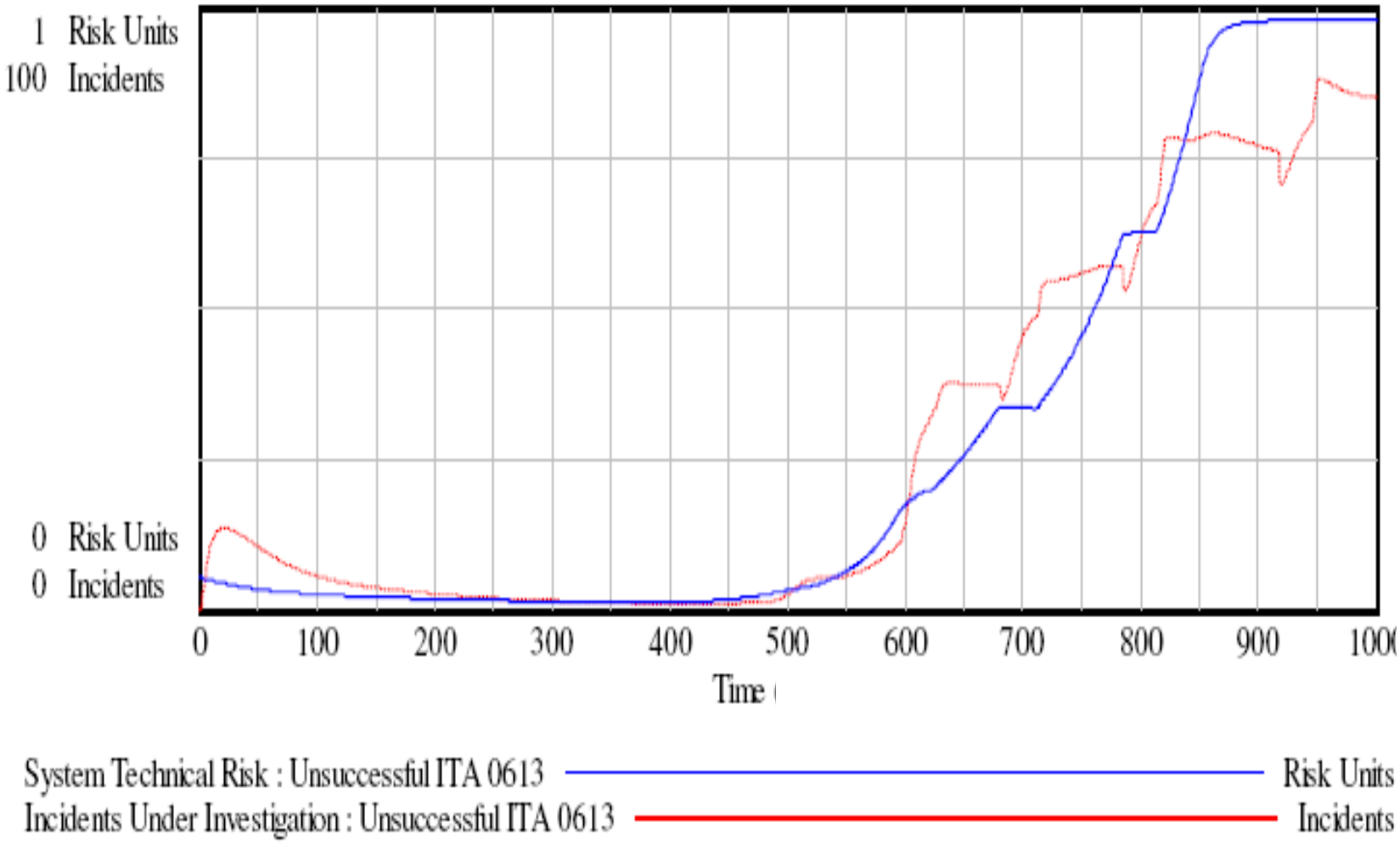
Unsuccessful Scenario Factors

- As effectiveness of ITA decreases, number of problems increase
  - Investigation requirements increase
  - Corners may be cut to compensate
    - Results in lower-quality investigation resolutions and corrective actions
  - TWHs and Trusted Agents become saturated and cannot attend to each investigation in timely manner
  - Bottleneck created by requiring TWHs to authorize all safety-related decisions, making things worse
- Want to detect this reinforcing loop while interventions still possible and not overly costly (resources, downtime)

Lagging vs. Leading Indicators

- Number of waivers issued good indicator but lags rapid increase in risk




1 Risk Units
100 Incidents
0 Risk Units
0 Incidents
0
100
200
300
400
500
600
700
800
900
1000
Time
System Technical Risk : Unsuccessful ITA 0613
Risk Units
Incidents Under Investigation : Unsuccessful ITA 0613
Incidents

Other Lagging Indicators

- Amount of resources available for safety activities
- Schedule pressure (only reduced when managers believe system unsafe)
- Perception of risk level by management (primarily affected by events and close-calls)

Monitoring leading indicators important because when reach tipping point (reinforcing loop has gain < 1), risk starts to increase very rapidly

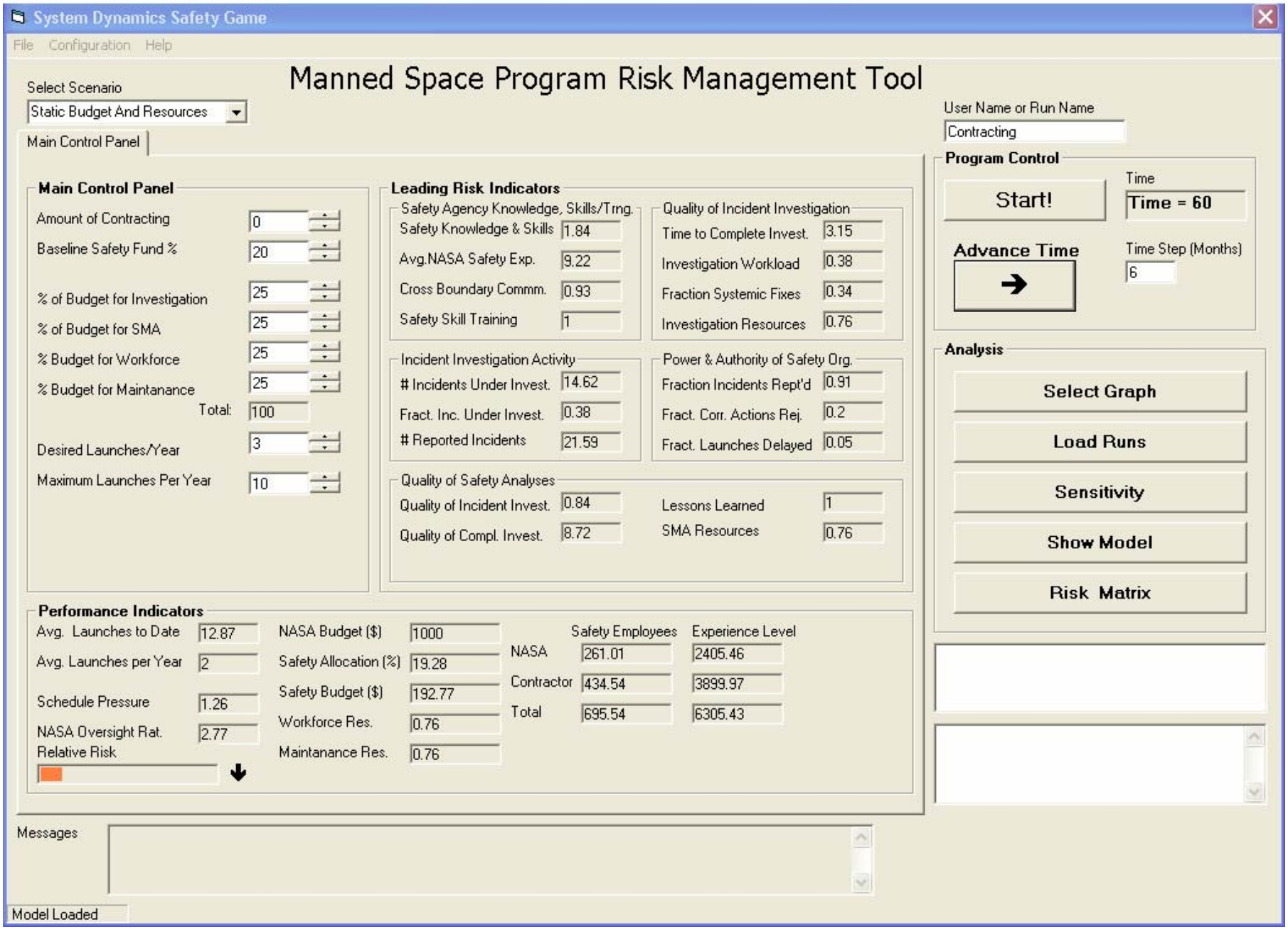
  - –Multiple problems start to occur
  - –Overwhelm problem-solving capacity of iTA

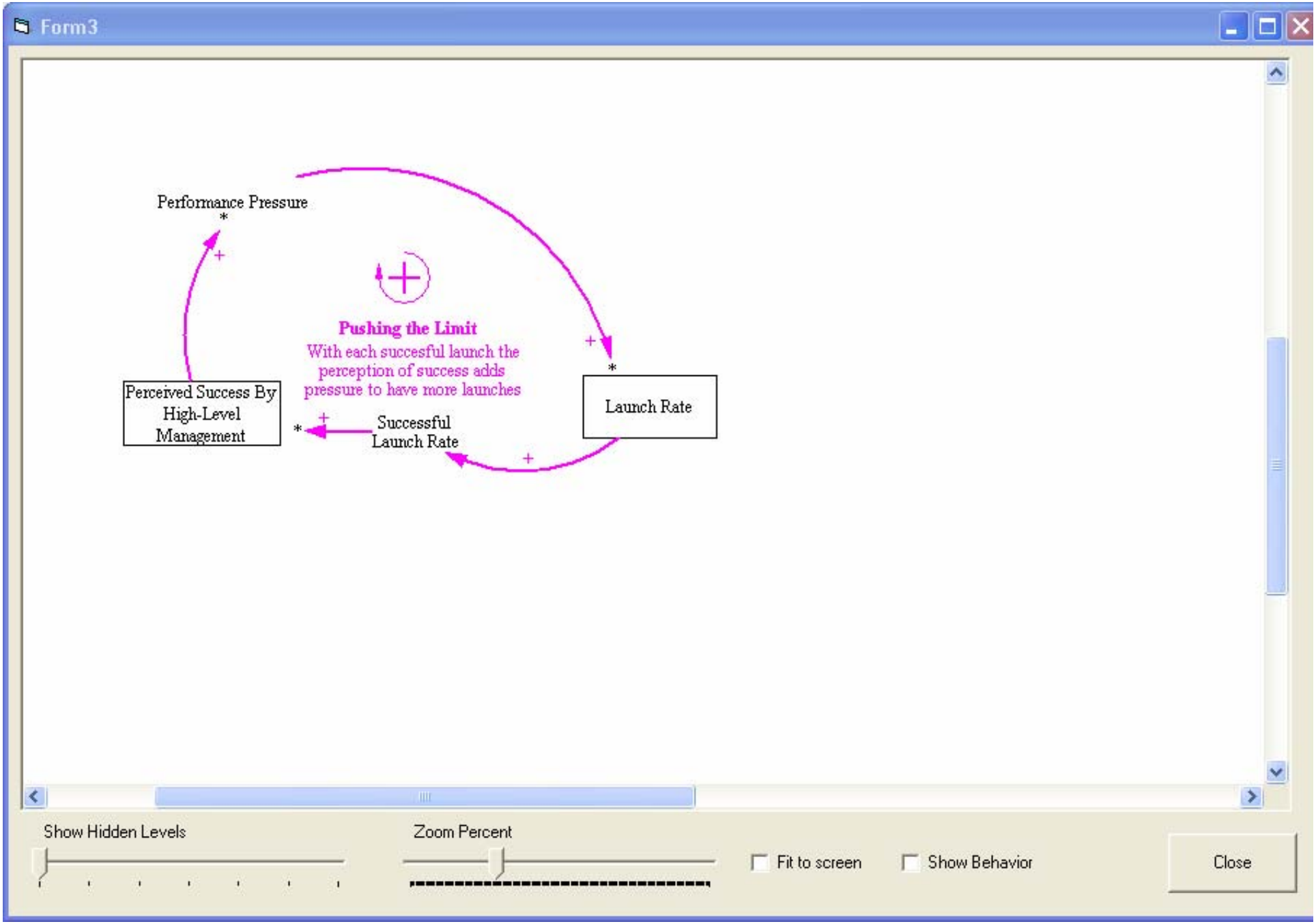
Leading Indicators

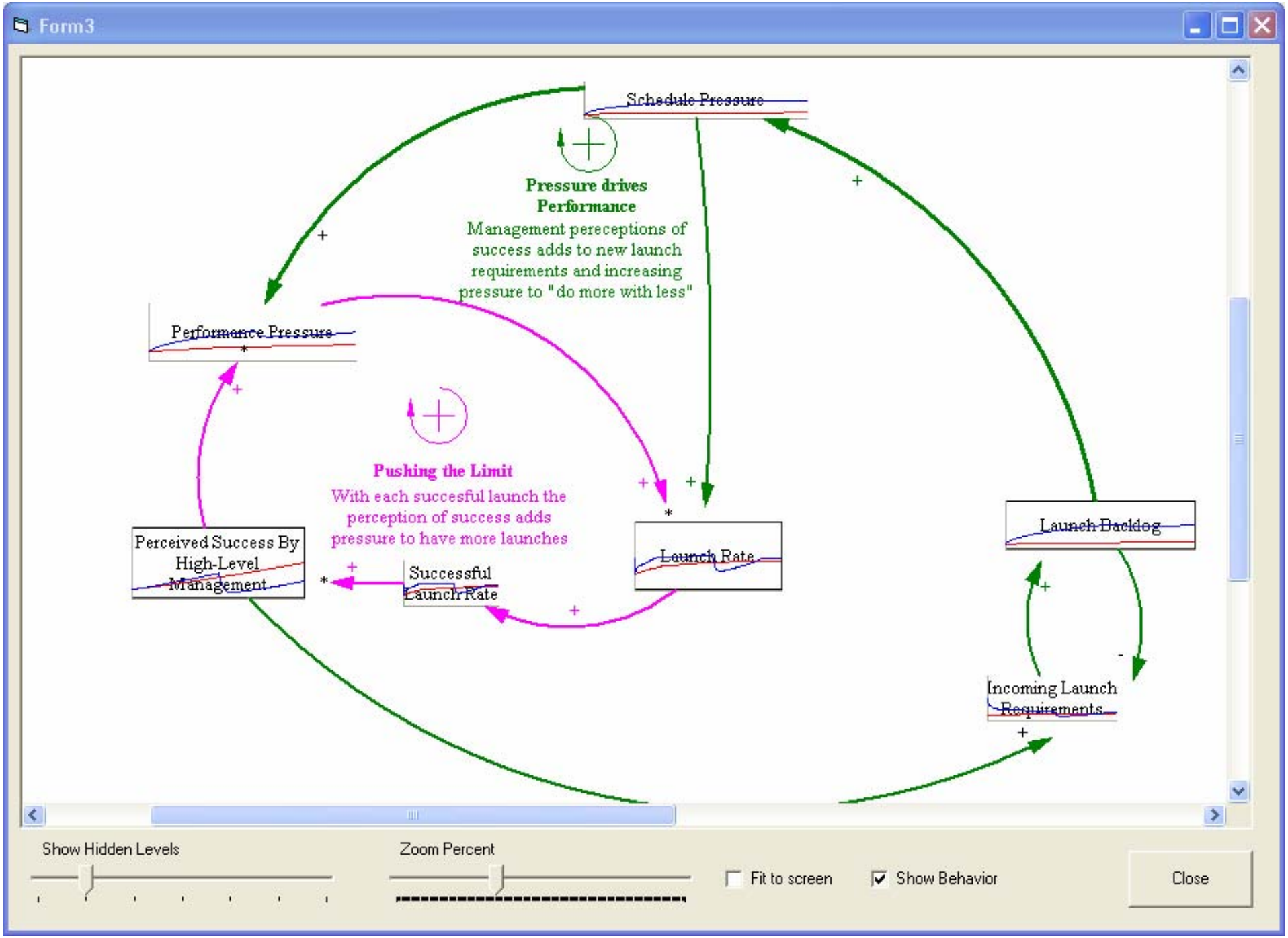
- Knowledge, skills, and quality of TWHs and Trusted Agents
  - Experience, technical knowledge, communication skills, reputation, social network, difficulty in recruiting replacements, amount of training
- ITA-directed investigation activity
  - Fraction of problem reports under ITA-directed investigation, number of unresolved or unhandled problems
- Quality of safety analyses
  - Knowledge and skills of safety staff, resources for safety analyses, availability of lessons learned

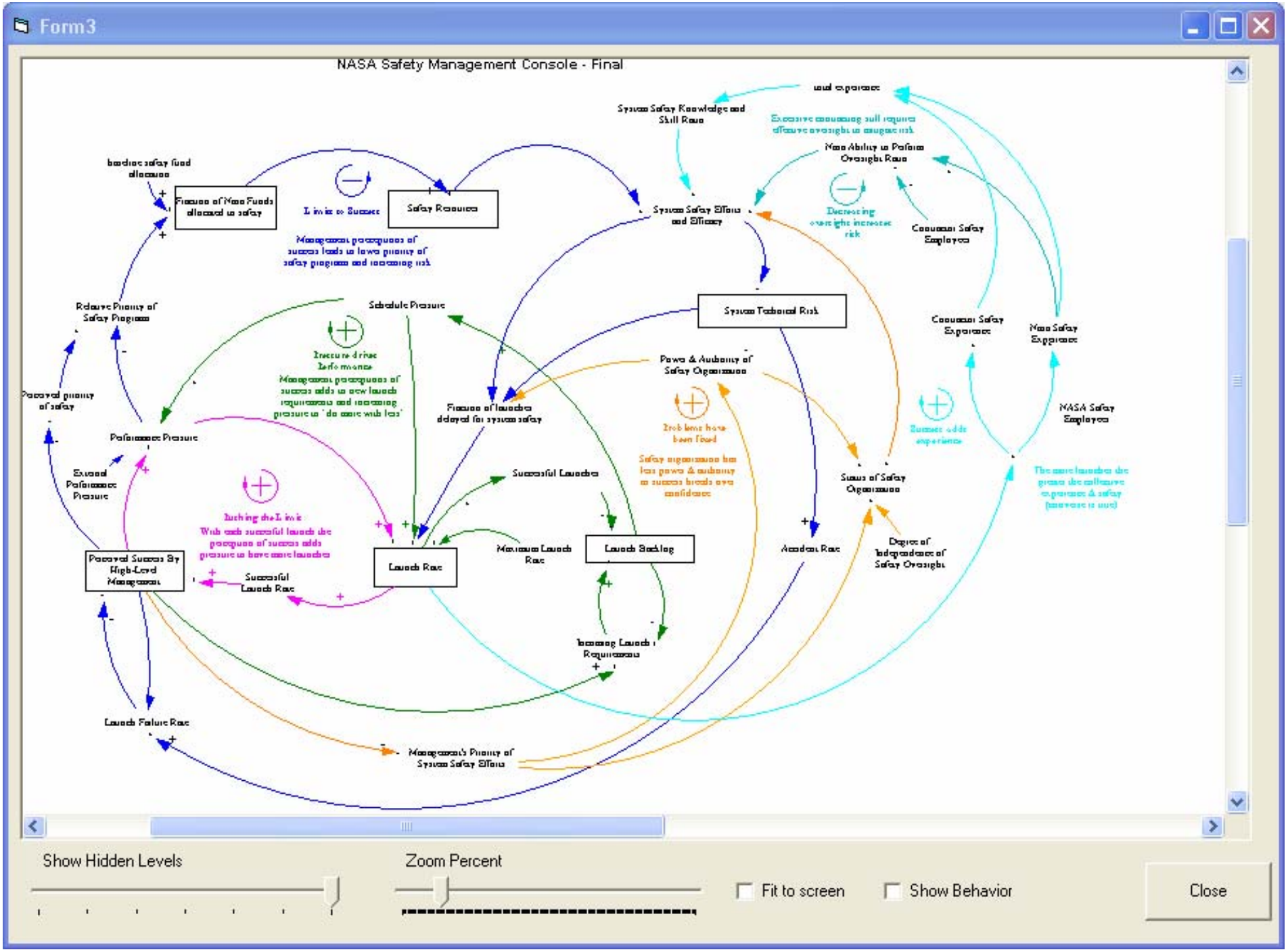
Leading Indicators (2)

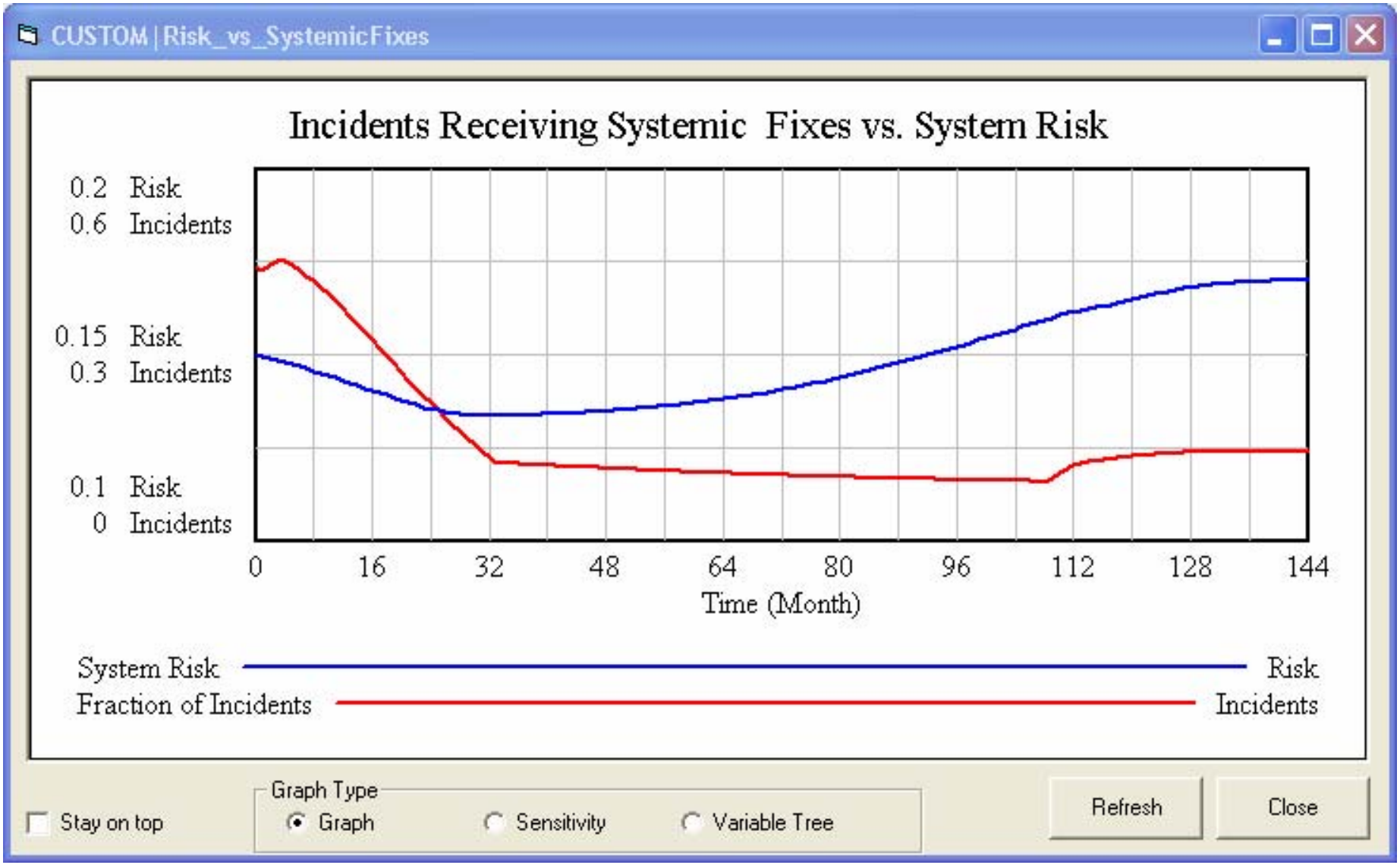
- Quality of incident investigation and fixes
  - Involvement of TWHs and TA (time, number), ITA investigation resources and workload, ITA independence and work balance, systemic factor fixes vs. symptom removal
- Power and authority of TWHs and Trusted Agents
  - Number of safety issues raised to ITA/Program level, fraction of rulings/decisions in favor of TWHs, number of launches delayed by ITA,

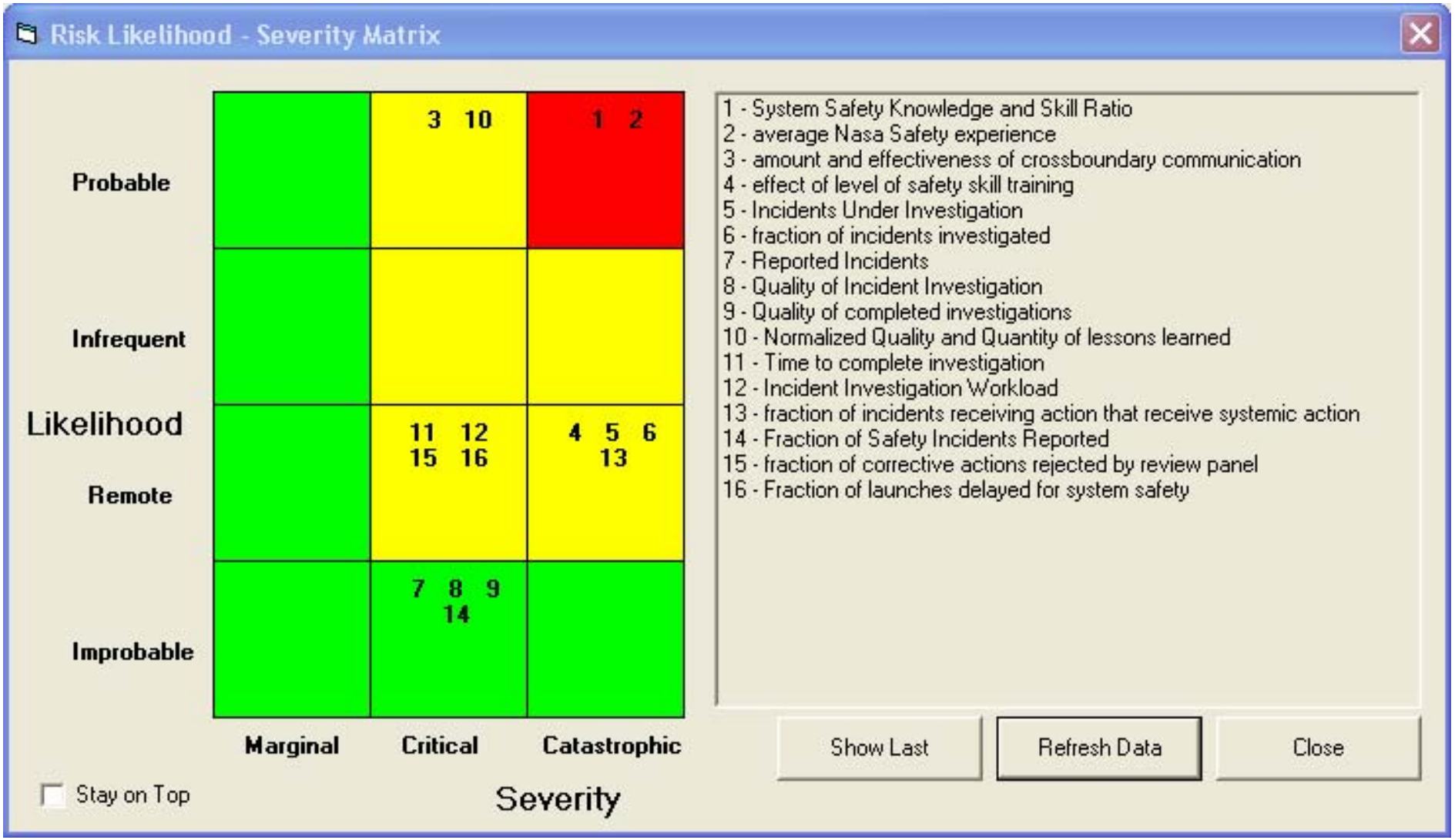

System Dynamics Safety Game
File Configuration Help
Manned Space Program Risk Management Tool
Select Scenario
Static Budget And Resources
User Name or Run Name
Contracting
Main Control Panel
Main Control Panel
Amount of Contracting 0
Baseline Safety Fund % 20
% of Budget for Investigation 25
% of Budget for SMA 25
% Budget for Workforce 25
% Budget for Maintanance 25
Total: 100
Desired Launches/Year 3
Maximum Launches Per Year 10
Leading Risk Indicators
Safety Agency Knowledge, Skills/Trng.
Safety Knowledge & Skills 1.84
Avg.NASA Safety Exp. 9.22
Cross Boundary Commm. 0.93
Safety Skill Training 1
Quality of Incident Investigation
Time to Complete Invest. 3.15
Investigation Workload 0.38
Fraction Systemic Fixes 0.34
Investigation Resources 0.76
Incident Investigation Activity
Incidents Under Invest. 14.62
Fract. Inc. Under Invest. 0.38
Reported Incidents 21.59
Power & Authority of Safety Org.
Fraction Incidents Rept'd 0.91
Fract. Corr. Actions Rej. 0.2
Fract. Launches Delayed 0.05
Quality of Safety Analyses
Quality of Incident Invest. 0.84
Quality of Compl. Invest. 8.72
Lessons Learned 1
SMA Resources 0.76
Program Control
Start!
Time
Time = 60
Advance Time
Time Step (Months) 6
Analysis
Select Graph
Load Runs
Sensitivity
Show Model
Risk Matrix
Performance Indicators
Avg. Launches to Date 12.87
Avg. Launches per Year 2
Schedule Pressure 1.26
NASA Oversight Rat. 2.77
Relative Risk
NASA Budget ($) 1000
Safety Allocation (%) 19.28
Safety Budget ($) 192.77
Workforce Res. 0.76
Maintanance Res. 0.76
Safety Employees
Experience Level
NASA 261.01 2405.46
Contractor 434.54 3899.97
Total 695.54 6305.43
Messages
Model Loaded


Form3
Performance Pressure
Pushing the Limit
With each succesful launch the perception of success adds pressure to have more launches
Perceived Success By High-Level Management
Successful Launch Rate
Launch Rate
Show Hidden Levels
Zoom Percent
Fit to screen
Show Behavior
Close


Form3
Schedule Pressure
Pressure drives Performance
Management pereceptions of success adds to new launch requirements and increasing pressure to "do more with less"
Performance Pressure
Pushing the Limit
With each succesful launch the perception of success adds pressure to have more launches
Perceived Success By High-Level Management
Successful Launch Rate
Launch Rate
Launch Backlog
Incoming Launch Requirements
Show Hidden Levels
Zoom Percent
Fit to screen
Show Behavior
Close


Form3
NASA Safety Management Console - Final
Fraction of New Funds allocated to safety
Safety Resource
Limits to Success
Management perceptions of success leads to lower priority of safety programs and increasing risk
System Safety Efforts and Efficacy
System Safety Knowledge and Skill Base
Excessive complacency will require offsetting oversight to mitigate risk
New Ability to Perform Oversight Base
Decreasing oversight increases risk
Cumulative Safety Experience
Relative Priority of Safety Programs
Schedule Pressure
System Technical Risk
Pressure driven Performance
Management perceptions of success adds to new launch requirements and increasing pressure to "do more with less"
Power & Authority of Safety Organization
Fraction of launches delayed for system safety
Problems have been found
Safety organization has less power & authority as success breeds over confidence
Success adds experience
New Safety Experience
NASA Safety Employee
Perceived priority of safety
Performance Pressure
Successful Launches
Extend Performance Pressure
Pushing the Limit
With each successful launch the perception of success adds pressure to have more launches
Status of Safety Organization
The more launches the greater the collective experience & safety (however is lost)
Perceived Success By High-Level Management
Launch Rate
Maximum Launch Rate
Launch Backlog
Accident Rate
Degree of Independence of Safety Oversight
Successful Launch Rate
Increasing Launch Requirements
Launch Failure Rate
Management's Priority of System Safety Efforts
Show Hidden Levels
Zoom Percent
Fit to screen
Show Behavior
Close


CUSTOM | Risk_vs_SystemicFixes
Incidents Receiving Systemic Fixes vs. System Risk
0.2 Risk
0.6 Incidents
0.15 Risk
0.3 Incidents
0.1 Risk
0 Incidents
0
16
32
48
64
80
96
112
128
144
Time (Month)
System Risk
Risk
Fraction of Incidents
Incidents
Stay on top
Graph Type
Graph
Sensitivity
Variable Tree
Refresh
Close


Risk Likelihood - Severity Matrix
Probable
Infrequent
Likelihood
Remote
Improbable
3 10
1 2
11 12
15 16
4 5 6
13
7 8 9
14
Marginal
Critical
Catastrophic
Severity
Stay on Top
1 - System Safety Knowledge and Skill Ratio
2 - average Nasa Safety experience
3 - amount and effectiveness of crossboundary communication
4 - effect of level of safety skill training
5 - Incidents Under Investigation
6 - fraction of incidents investigated
7 - Reported Incidents
8 - Quality of Incident Investigation
9 - Quality of completed investigations
10 - Normalized Quality and Quantity of lessons learned
11 - Time to complete investigation
12 - Incident Investigation Workload
13 - fraction of incidents receiving action that receive systemic action
14 - Fraction of Safety Incidents Reported
15 - fraction of corrective actions rejected by review panel
16 - Fraction of launches delayed for system safety
Show Last
Refresh Data
Close

Conclusions

- Our rigorous approach to risk analysis is practical and provides useful results
  - Recommendations for policy and structural changes in the manned space program
  - Set of leading indicators of increasing risk to detect drift toward accidents
  - Insight into causal factors behind risk in the NASA manned space program and the factors involved in the Challenger and Columbia accidents
- Tool set will allow engineers and managers to build the models and use them for engineering and management decision making
  - Currently developing techniques to automatically generate system dynamics models
  - Building models for risk management in ESMD